Adversarial Texture for Fooling Person Detectors in the Physical World

Year: 2022 | Citations: 142 | Authors: Zhan Hu, Siyuan Huang, Xiaopei Zhu, Xiaolin Hu, Fuchun Sun

Abstract

Nowadays, cameras equipped with AI systems can capture and analyze images to detect people automatically. However, the AI system can make mistakes when receiving deliberately designed patterns in the real world, i.e., physical adversarial examples. Prior works have shown that it is possible to print adversarial patches on clothes to evade DNN-based person detectors. However, these adversarial examples could have catastrophic drops in the attack success rate when the viewing angle (i.e., the camera's angle towards the object) changes. To perform a multi-angle attack, we propose Adversarial Texture (AdvTexture). AdvTexture can cover clothes with arbitrary shapes so that people wearing such clothes can hide from person detectors from different viewing angles. We propose a generative method, named Toroidal-Cropping-based Expandable Generative Attack (TC-EGA), to craft AdvTexture with repetitive structures. We printed several pieces of cloth with AdvTexure and then made T-shirts, skirts, and dresses in the physical world. Experiments showed that these clothes could fool person detectors in the physical world.